PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-157040
(43)Date of publication of application : 31.05.2002

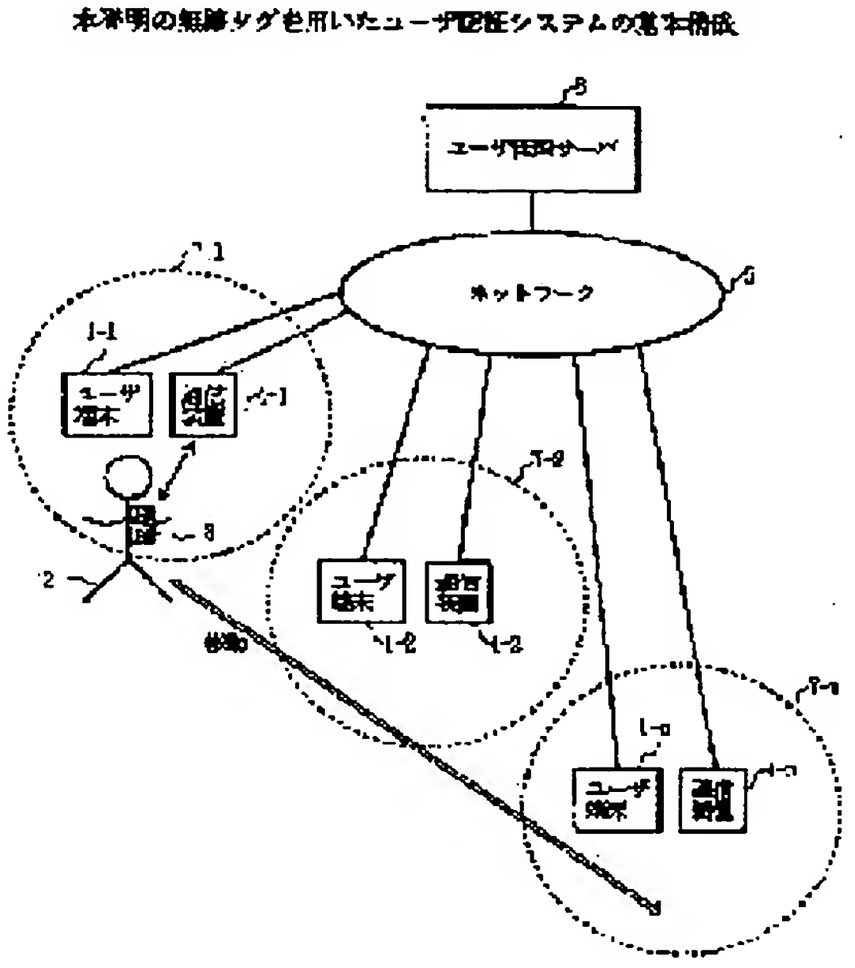
(51)Int.CI. G06F 1/00
G06F 1/26
G06F 15/00
G06K 17/00
G06K 19/07
G06K 19/00
H04L 9/32

(21)Application number : 2000-355466
(22)Date of filing : 22.11.2000

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : ONO YUKIHARU
OKA MASAHIKO
MIKAZUKI TETSUO

(54) USER AUTHENTICATION METHOD AND USER AUTHENTICATION SYSTEM USING RADIO TAG

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a working environment according to a user by automatically performing the stating of a terminal close to a radio tag carried by the user and the authentication of the user by the communication with the wireless tag in an indoor or filed environment where a plurality of terminals (personal computers) of general specification are arranged.
SOLUTION: In this user authentication method for performing the authentication of the user using a user terminal between at least one user terminal arranged in a room or field and a user management server connected to each user terminal through a network, a communication device arranged in the vicinity of each user terminal receives identification data for the user by the communication with the radio tag carried by the user, and transmits the identification data to the user management server through the network. The user management server authenticates the transferred identification data, and performs a starting control for turning ON the power supply of the user terminal in the vicinity of the communication device for which the identification data is received.



LEGAL STATUS

[Date of request for examination] 24.07.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００２－１５７０４０
（Ｐ２００２－１５７０４０Ａ）
(43)公開日　平成14年5月31日(2002.5.31)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	1/00	３７０	Ｇ０６Ｆ	1/00	３７０ Ｅ	5B011
	1/26			15/00	３３０ Ｇ	5B035
	15/00	３３０	Ｇ０６Ｋ	17/00	Ｆ	5B058
Ｇ０６Ｋ	17/00				Ｖ	5B085
			Ｇ０６Ｆ	1/00	３３４ Ｊ	5J104

審査請求　未請求　請求項の数８　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願2000-355466(P2000-355466)

(22)出願日　平成12年11月22日(2000.11.22)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72)発明者　大野　幸春
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内
(72)発明者　岡　正彦
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内
(74)代理人　100072718
弁理士　古谷　史旺

最終頁に続く

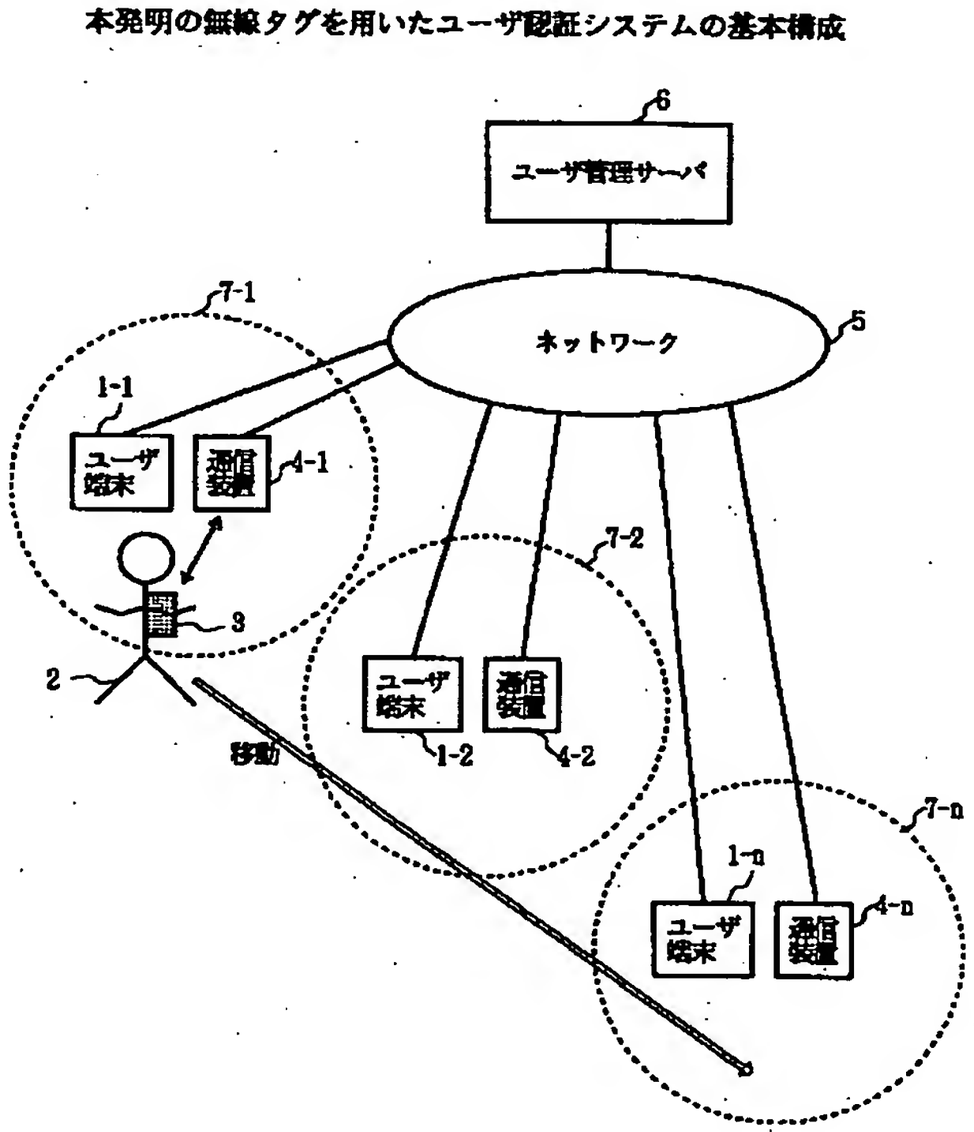
(54)【発明の名称】無線タグを用いたユーザ認証方法およびユーザ認証システム

(57)【要約】

【課題】　複数の通常仕様の端末（パソコン）が配置される室内またはフィールド環境において、ユーザが携帯する無線タグとの交信により、接近した端末の起動およびユーザ認証を自動的に行い、ユーザに応じた作業環境を提供する。

【解決手段】　室内またはフィールドに配置した１台以上のユーザ端末と、各ユーザ端末とネットワークを介して接続されるユーザ管理サーバとの間で、ユーザ端末を利用するユーザの認証を行うユーザ認証方法において、各ユーザ端末の近傍に配置された通信装置が、ユーザの携帯する無線タグとの交信によりユーザの識別データを受信し、通信装置から識別データをネットワークを介してユーザ管理サーバに転送し、ユーザ管理サーバが転送された識別データの認証を行い、その識別データを受信した通信装置の近傍のユーザ端末の電源をオンとする起動制御を行う。

本発明の無線タグを用いたユーザ認証システムの基本構成



【特許請求の範囲】

【請求項１】　室内またはフィールドに配置した１台以上のユーザ端末と、各ユーザ端末とネットワークを介して接続されるユーザ管理サーバとの間で、前記ユーザ端末を利用するユーザの認証を行うユーザ認証方法において、

前記各ユーザ端末の近傍に配置された通信装置が、ユーザの携帯する無線タグとの交信によりユーザの識別データを受信し、

前記通信装置から前記識別データを前記ネットワークを介して前記ユーザ管理サーバに転送し、

前記ユーザ管理サーバが転送された識別データの認証を行い、その識別データを受信した通信装置の近傍のユーザ端末の電源をオンとする起動制御を行うことを特徴とする無線タグを用いたユーザ認証方法。

【請求項２】　請求項１に記載の無線タグを用いたユーザ認証方法において、

前記ユーザ管理サーバは、前記ユーザが認証を受けたユーザ端末から離れたことを検出したときに、そのユーザ端末の認証離脱および電源をオフとする起動停止制御を行うことを特徴とする無線タグを用いたユーザ認証方法。

【請求項３】　請求項１または請求項２に記載の無線タグを用いたユーザ認証方法において、

前記ユーザ管理サーバは、起動制御を行うユーザ端末に対して、認証した識別データを有するユーザに対応する操作環境を設定することを特徴とする無線タグを用いたユーザ認証方法。

【請求項４】　請求項３に記載の無線タグを用いたユーザ認証方法において、

前記ユーザ管理サーバは、ユーザが前記ユーザ端末間を移動したときに、移動前のユーザ端末に設定されていた操作環境を引き続いて移動後のユーザ端末に設定することを特徴とする無線タグを用いたユーザ認証方法。

【請求項５】　室内またはフィールドに配置した１台以上のユーザ端末と、各ユーザ端末とネットワークを介して接続されるユーザ管理サーバとの間で、前記ユーザ端末を利用するユーザの認証を行うユーザ認証システムにおいて、

前記各ユーザ端末の近傍に配置され、ユーザが携帯する無線タグとの交信によりユーザの識別データを受信し、その識別データを前記ネットワークを介して前記ユーザ管理サーバに転送する通信装置を備え、

前記ユーザ管理サーバは、転送された識別データの認証を行い、その識別データを受信した通信装置の近傍のユーザ端末の電源をオンとする起動制御を行う構成であることを特徴とする無線タグを用いたユーザ認証システム。

【請求項６】　請求項５に記載の無線タグを用いたユーザ認証システムにおいて、

前記ユーザ管理サーバは、前記ユーザが認証を受けたユーザ端末から離れたことを検出したときに、そのユーザ端末の認証離脱および電源をオフとする起動停止制御を行う構成であることを特徴とする無線タグを用いたユーザ認証システム。

【請求項７】　請求項５または請求項６に記載の無線タグを用いたユーザ認証システムにおいて、

前記ユーザ管理サーバは、起動制御を行うユーザ端末に対して、認証した識別データを有するユーザに対応する操作環境を設定する構成であることを特徴とする無線タグを用いたユーザ認証システム。

【請求項８】　請求項５または請求項６に記載の無線タグを用いたユーザ認証システムにおいて、

前記各ユーザ端末の近傍に配置され、前記ユーザの接近を検知し、その検知信号を前記ネットワークを介して前記ユーザ管理サーバに転送するセンサを備え、

前記ユーザ管理サーバは、前記検知信号により前記センサの近傍の通信装置の電源をオンとし前記無線タグとの交信を開始する制御を行う構成であることを特徴とする無線タグを用いたユーザ認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の端末が配置される室内またはフィールド環境において、ユーザが任意の端末を利用する際に、各端末ごとにユーザの認証を自動的に行う無線タグを用いたユーザ認証方法およびユーザ認証システムに関する。

【０００２】

【従来の技術】端末の使用に際してユーザを識別し、認証されたユーザのみが使用できるようにしたセキュリティシステムが提案されている。

【０００３】例えば、特開平９－２４５１３８号公報（名札及びセキュリティ端末並びにこれらを利用したセキュリティシステム）に記載のシステムは、ユーザが個人の識別データを記録した無線タグを携帯し、外部のセキュリティ端末から周期的に照合要求信号を送信し、それを受信した無線タグが応答する識別データをセキュリティ端末が認証し、起動を許可する構成である。これにより、ユーザは特別な操作を行うことなく、高いセキュリティが実現するというものである。

【０００４】

【発明が解決しようとする課題】上記の公報に記載されているような従来のセキュリティシステムは、特別仕様のセキュリティ制御部を備えた端末が必要であり、一般的な市販のパソコンをそのままシステム内に組み入れることはできなかった。

【０００５】また、例えばフィールドにおける環境情報収集作業において、ユーザが観察ポイントを順次移動する場合に、それぞれの観察ポイントに配備した端末が次々とユーザを自動的に識別し、各ユーザに対応した適切

なアプリケーションを起動し、さらに各ユーザが必要とするデータを表示装置に表示するようなシステムが望まれている。しかし、従来のセキュリティシステムは、ユーザが移動しながら複数の端末を使用するような状況は想定されていなかった。さらに、従来のセキュリティシステムはスタンドアロン環境に限られ、セキュリティ制御部をネットワークを介してサーバで集中的に管理できるような構成になっていなかった。このような集中管理が可能であれば、例えばユーザＩＤから端末ＩＤへのデータ変換が実現でき、ユーザの移動に伴って各ポイントの端末に処理を引き渡すことも可能となる。

【０００６】本発明は、複数の通常仕様の端末（パソコン）が配置される室内またはフィールド環境において、ユーザが携帯する無線タグとの交信により、接近した端末の起動およびユーザ認証を自動的に行い、ユーザに応じた作業環境を提供する無線タグを用いたユーザ認証方法およびユーザ認証システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の無線タグを用いたユーザ認証方法は、室内またはフィールドに配置した１台以上のユーザ端末と、各ユーザ端末とネットワークを介して接続されるユーザ管理サーバとの間で、ユーザ端末を利用するユーザの認証を行うユーザ認証方法において、各ユーザ端末の近傍に配置された通信装置が、ユーザの携帯する無線タグとの交信によりユーザの識別データを受信し、通信装置から識別データをネットワークを介してユーザ管理サーバに転送し、ユーザ管理サーバが転送された識別データの認証を行い、その識別データを受信した通信装置の近傍のユーザ端末の電源をオンとする起動制御を行う。

【０００８】また、ユーザ管理サーバは、ユーザが認証を受けたユーザ端末から離れたことを検出したときに、そのユーザ端末の認証離脱および電源をオフとする起動停止制御を行うようにしてもよい。また、ユーザ管理サーバは、起動制御を行うユーザ端末に対して、認証した識別データを有するユーザに対応する操作環境を設定するようにしてもよい。さらに、ユーザ管理サーバは、ユーザがユーザ端末間を移動したときに、移動前のユーザ端末に設定されていた操作環境を引き続いて移動後のユーザ端末に設定するようにしてもよい。

【０００９】本発明の無線タグを用いたユーザ認証システムは、室内またはフィールドに配置した１台以上のユーザ端末と、各ユーザ端末とネットワークを介して接続されるユーザ管理サーバとの間で、ユーザ端末を利用するユーザの認証を行うユーザ認証システムにおいて、各ユーザ端末の近傍に配置され、ユーザが携帯する無線タグとの交信によりユーザの識別データを受信し、その識別データをネットワークを介してユーザ管理サーバに転送する通信装置を備え、ユーザ管理サーバは、転送された識別データの認証を行い、その識別データを受信した通信装置の近傍のユーザ端末の電源をオンとする起動制御を行う構成である。

【００１０】また、ユーザ管理サーバは、ユーザが認証を受けたユーザ端末から離れたことを検出したときに、そのユーザ端末の認証離脱および電源をオフとする起動停止制御を行う構成としてもよい。また、ユーザ管理サーバは、起動制御を行うユーザ端末に対して、認証した識別データを有するユーザに対応する操作環境を設定する構成としてもよい。

【００１１】さらに、各無線端末の近傍でユーザの接近を検知し、その検知信号をネットワークを介してユーザ管理サーバに転送するセンサを備え、ユーザ管理サーバは、検知信号によりセンサの近傍の通信装置の電源をオンとし無線タグとの交信を開始する制御を行う構成としてもよい。

【００１２】

【発明の実施の形態】（基本構成）図１は、本発明の無線タグを用いたユーザ認証システムの基本構成を示す。図において、室内またはフィールドには複数台のユーザ端末１－１～１－ｎが配置される。ユーザ２は、個人の識別データを記録した無線タグ３を携帯し、室内またはフィールドを移動する。各ユーザ端末１－１～１－ｎの近傍には、ユーザ２が携帯する無線タグ３と交信する通信装置４－１～４－ｎが配置される。各ユーザ端末１－１～１－ｎおよび各通信装置４－１～４－ｎは、ＬＡＮ，ＰＨＳ，インターネット等のネットワーク５を介してユーザ管理サーバ６に接続される。

【００１３】ここで、無線タグ３は、ユーザ２の名札の中に組み込まれる形状や、ＩＣカードのような形状などいずれでもよい。通信装置４－１～４－ｎの周辺には、それぞれ無線タグ３との通信圏となるエリア７－１～７－ｎが形成される。例えば、エリア７－１内にユーザ２が入ると、無線タグ３と通信装置４－１との間で識別データが送受信され、その識別データがネットワーク５を介してユーザ管理サーバ６に転送されて認証が行われる。ユーザ管理サーバ６は、この認証により対応するユーザ端末１－１の電源をオンとし、対応するアプリケーションを起動する。また、ユーザ２がこのエリア７－１から遠ざかると、通信装置４－１が無線タグ３との通信途絶を検出してユーザ管理サーバ６に通知し、そのユーザ端末１－１の認証離脱を行って電源をオフにする。

【００１４】（第１の実施形態）図２は、本発明の無線タグを用いたユーザ認証システムの第１の実施形態を示す。図において、ユーザ端末１、ユーザ２が携帯する無線タグ３、通信装置４を構成する人体センサ４１とリーダライタ４２とプロトコル変換器４３、ネットワーク５を構成するイーサネット５１、ユーザ管理サーバ６は、図１に示す基本構成のものと対応する。なお、人体センサ４１は、赤外線を用いた感熱センサまたは距離センサ

などによりユーザ２の接近を検知する。リーダライタ４２は、無線タグ３との交信によりユーザ２の識別データを読み取る。プロトコル変換器４３は、リーダライタ４２とイーサネット５１とを接続する。

【００１５】なお、識別データは、ユーザ端末１を利用する際に必要なユーザアカウント名やパスワードなどを含む情報である。その他、例えば学年情報などの包括的な情報が付加される場合もある。さらに、セキュリティ向上を考慮すると、ユーザ管理サーバ６におけるユーザアカウント名やパスワードと、ユーザ端末１におけるユーザアカウント名やパスワードを別々とし、識別データとしてそれぞれ複数のユーザアカウント名やパスワードを利用するようにしてもよい。

【００１６】図３は、ユーザの接近によるユーザ端末起動までの動作手順を示す。図２および図３において、ユーザ２がユーザ端末１に接近すると（Ｓ１）、ユーザ端末１の近傍に配置した人体センサ４１がユーザ２の接近を検知し（Ｓ２）、イーサネット（登録商標）５１を介してユーザ管理サーバ６に通知する。ユーザ管理サーバ６はユーザ２の接近通知により、イーサネット５１およびプロトコル変換器４３を介してリーダライタ４２の電源をオンにする（Ｓ３）。リーダライタ４２は、ユーザ２が携帯する無線タグ３との交信によりユーザ２の識別データを受信し、プロトコル変換器４３およびイーサネット５１を介してユーザ管理サーバ６に通知する（Ｓ４）。

【００１７】ユーザ管理サーバ６は、通知された識別データについて、予め登録された各ユーザの使用許諾に関するデータベースを参照して比較し、正規のユーザと認める場合には、イーサネット５１を介してユーザ端末１の電源をオンとし、アプリケーションのログインを実行するコマンドを送信する（Ｓ５，Ｓ６）。なお、ユーザ端末１の起動制御には、例えばWake on LAN ボードを用いることができる。

【００１８】図４は、ユーザの離脱によるユーザ端末起動停止までの動作手順を示す。図２および図４において、ユーザ２がユーザ端末１から遠ざかると（Ｓ11）、無線タグ３との定期的な交信を行っているリーダライタ４２が、規定時間を越えた通信途絶によりユーザ離脱を検出し（Ｓ12）、イーサネット５１を介してユーザ管理サーバ６に通知する。ユーザ管理サーバ６はユーザ２の認証離脱を行い（Ｓ13）、イーサネット５１を介してユーザ端末１のアプリケーションを終了し、電源をオフとするコマンドを送信する（Ｓ14，Ｓ15）。

【００１９】なお、他にユーザ離脱を検出する簡便な方法としては、全てのユーザ端末を短時間でサスペンド状態になるように設定しておき、それを眠りから覚ます場合に再度認証を要求する構成により対応できる。この機能はＷｉｎｄｏｗｓ（登録商標）　９８　Ｓｅｃｏｎｄ　Ｅｄｉｔｉｏｎ　に標準搭載されている。

【００２０】また、ユーザ２が他のユーザ端末１に移動する場合には、同様の手順により新規のユーザ端末１に対する新規の認証処理を行う。この場合には、ユーザ管理サーバ６に移動したことを示すデータが残るので、二重ログインを防止する制御も可能である。

【００２１】さらに、本システムは付加機能として、ユーザ２の識別データからそのユーザに対応するアプリケーションを自動的に起動するような制御も可能である。また、そのユーザ２が必要とするデータを起動したアプリケーション中に表示させる制御も可能である。また、ユーザ２が使用したアプリケーションおよびその作業内容をユーザ管理サーバ６で監視し、ユーザ２の作業データの変更に関してログを記録することにより、ユーザ２が他のユーザ端末１に移動した場合でも、作業を継続して行うことができる操作環境を実現することができる。

【００２２】（第２の実施形態）図５は、本発明の無線タグを用いたユーザ認証システムの第２の実施形態を示す。図において、ユーザ端末１－１～１－８、ユーザ２が携帯する無線タグ３、通信装置４を構成するリーダライタ４２－１～４２－８、ネットワーク５を構成するイーサネット５１およびＲＳ－２３２Ｃ５２、ユーザ管理サーバ６は、図１に示す基本構成のものと対応する。なお、イーサネット５１は、ユーザ端末１－１～１－８とユーザ管理サーバ６とを接続し、ＲＳ－２３２Ｃ（８ポート分岐）５２は、リーダライタ４２－１～４２－８とユーザ管理サーバ６とを接続する。

【００２３】ユーザ２がユーザ端末１－１に接近すると、ユーザ端末１－１の近傍に配置したリーダライタ４２－１とユーザ２が携帯する無線タグ３が通信可能となる。リーダライタ４２－１は、無線タグ３との通信によりユーザ２の識別データを読み取り、ＲＳ－２３２Ｃ５２を介してユーザ管理サーバ６に通知する。なお、ＲＳ－２３２Ｃ（８ポート分岐）５２は、８台までのリーダライタ４２－１～４２－８を１台のユーザ管理サーバ６で管理・制御できる特徴があるが、他にＵＳＢ、ＰＣＭＣＩＡなどのインタフェースを用いてもよい。

【００２４】ユーザ管理サーバ６は、通知された識別データについて、予め登録された各ユーザの使用許諾に関するデータベースを参照して比較し、正規のユーザと認める場合には、イーサネット５１を介してユーザ端末１－１の電源をオンとし、アプリケーションのログインを実行するコマンドを送信する。

【００２５】ユーザ２がユーザ端末１－１から遠ざかると、無線タグ３との定期的な交信を行っているリーダライタ４２－１が、規定時間を越えた通信途絶によりユーザ離脱を検出し、ＲＳ－２３２Ｃ５２を介してユーザ管理サーバ６に通知する。ユーザ管理サーバ６はユーザ２の認証離脱を行い、イーサネット５１を介してユーザ端末１－１のアプリケーションを終了し、電源をオフとするコマンドを送信する。

【００２６】（第３の実施形態）図６は、本発明の無線タグを用いたユーザ認証システムの第３の実施形態を示す。図において、ユーザ端末１、ユーザ２が携帯する無線タグ３、通信装置４を構成するリーダライタ４２、ネットワーク５を構成する構内ＰＨＳ網５３、ユーザ管理サーバ６は、図１に示す基本構成のものと対応する。

【００２７】本実施形態は、ネットワーク５として第１の実施形態におけるイーサネット５１、第２の実施形態におけるイーサネット５１およびＲＳ－２３２Ｃ（８ポート分岐）５２に代わるものであり、ユーザ端末１およびリーダライタ４２とユーザ管理サーバ６との間を接続する形態の変更例である。ユーザ２の接近検出から認証およびユーザ端末１の起動制御などの動作手順は、第１の実施形態および第２の実施形態と同様である。

【００２８】（第４の実施形態）図７は、本発明の無線タグを用いたユーザ認証システムの第４の実施形態を示す。図において、ユーザ端末１、ユーザ２が携帯する無線タグ３、通信装置４を構成するリーダライタ４２、ネットワーク５を構成するＳＳ無線ＬＡＮ５４、ユーザ管理サーバ６は、図１に示す基本構成のものと対応する。

【００２９】本実施形態は、第３の実施形態の構内ＰＨＳ網５３をＳＳ無線ＬＡＮ５４に代えたものであり、ユーザ端末１およびリーダライタ４２とユーザ管理サーバ６との間を接続する形態の変更例である。ユーザ２の接近検出から認証およびユーザ端末１の起動制御などの動作手順は、第１の実施形態および第２の実施形態と同様である。

【００３０】（第５の実施形態）図８は、本発明の無線タグを用いたユーザ認証システムの第５の実施形態を示す。図において、ユーザ端末１、ユーザ２が携帯する無線タグ３、通信装置４を構成するリーダライタ４２、ネットワーク５を構成するインターネット５５、ユーザ管理サーバ６は、図１に示す基本構成のものと対応する。

【００３１】本実施形態は、第３の実施形態の構内ＰＨＳ網５３をインターネット５５に代えたものであり、ユーザ端末１およびリーダライタ４２とユーザ管理サーバ６との間を接続する形態の変更例である。ユーザ２の接近検出から認証およびユーザ端末１の起動制御などの動作手順は、第１の実施形態および第２の実施形態と同様である。

【００３２】（第６の実施形態）図９は、本発明の無線タグを用いたユーザ認証システムの第６の実施形態を示す。ここでは、ユーザ認証により、ユーザごとに最適なアプリケーションやデータベースの動作および表示環境を行う例を示す。図において、ユーザ端末１、ユーザ２－１～２－３が携帯する無線タグ３、通信装置４、ネットワーク５、ユーザ管理サーバ６は、図１に示す基本構成のものと対応する。

【００３３】ここで、小学校においてフィールド環境調査の授業を行う場合に、各学年ごとにユーザ端末１に表示される調査項目、質問内容等を自動的に変更することを想定する。ユーザ２－１は小学１年生、ユーザ２－２は小学３年生、ユーザ２－３は小学６年生とする。それぞれのユーザには、予めそれぞれの学年に相当する識別データを記録した無線タグ３を携帯させておく。

【００３４】ユーザ２－１がユーザ端末１に接近すると、ユーザ端末１の近傍に配置した通信装置４とユーザ２－１が携帯する無線タグ３が通信可能となる。通信装置４は、無線タグ３との交信によりユーザ２－１の識別データ（小学１年生）を読み取り、ネットワーク５を介してユーザ管理サーバ６に通知する。ユーザ管理サーバ６は、通知された識別データについて、予め登録された各ユーザの使用許諾に関するデータベースを参照して比較し、正規のユーザと認める場合には、ネットワーク５を介してユーザ端末１の電源をオンとし、小学１年生向けのアプリケーションを起動する。さらに、そのアプリケーションの内部データベースや、環境教育授業における質問、助言などの情報をユーザ端末１の画面に表示する。他の学年のユーザが接近したときも同様である。

【００３５】

【発明の効果】以上説明したように、本発明の無線タグを用いたユーザ認証方法およびユーザ認証システムは、室内またはフィールドに複数配置したユーザ端末の認証作業を容易かつ自動的に行うことができる。しかも、ユーザ端末に特別な認証回路が不要であり、ユーザ端末数やユーザ数に制限ないユーザ認証システムを実現することができる。さらに、ユーザの接近および認証により、無線タグとの交信用の通信装置やユーザ端末の電源のオンオフ制御が行われるので、省電力化を図ることができる。

【００３６】さらに、ユーザが接近したユーザ端末に、各ユーザに応じた操作環境を設定することができ、またユーザ端末間の移動でもその操作環境を継続させることが可能となるので、極めて利便性の高いシステムを構成することができる。例えば、ユーザごとにアプリケーションおよびデータへのアクセスを自動的に選別し、ユーザごとに最適環境を提供することが可能となる。

【図面の簡単な説明】

【図１】本発明の無線タグを用いたユーザ認証システムの基本構成を示す図。

【図２】本発明の無線タグを用いたユーザ認証システムの第１の実施形態を示す図。

【図３】ユーザの接近によるユーザ端末起動までの動作手順を示すフローチャート。

【図４】ユーザの離脱によるユーザ端末起動停止までの動作手順を示すフローチャート。

【図５】本発明の無線タグを用いたユーザ認証システムの第２の実施形態を示す図。

【図６】本発明の無線タグを用いたユーザ認証システムの第３の実施形態を示す図。

【図７】本発明の無線タグを用いたユーザ認証システムの第４の実施形態を示す図。

【図８】本発明の無線タグを用いたユーザ認証システムの第５の実施形態を示す図。

【図９】本発明の無線タグを用いたユーザ認証システムの第６の実施形態を示す図。

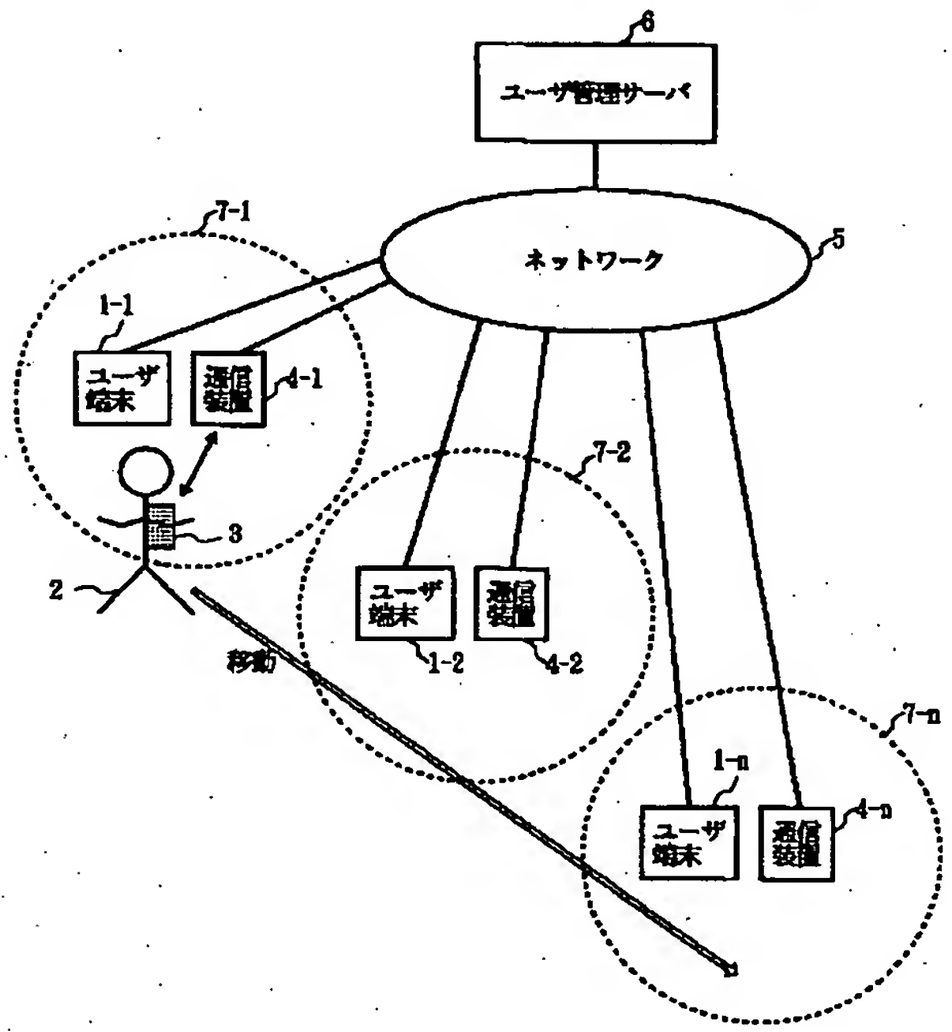
【符号の説明】

１　ユーザ端末
２　ユーザ
３　無線タグ
４　通信装置

５　ネットワーク
６　ユーザ管理サーバ
７　エリア
４１　人体センサ
４２　リーダライタ
４３　プロトコル変換器
５１　イーサネット
５２　ＲＳ－２３２Ｃ
５３　構内ＰＨＳ網
５４　ＳＳ無線ＬＡＮ
５５　インターネット

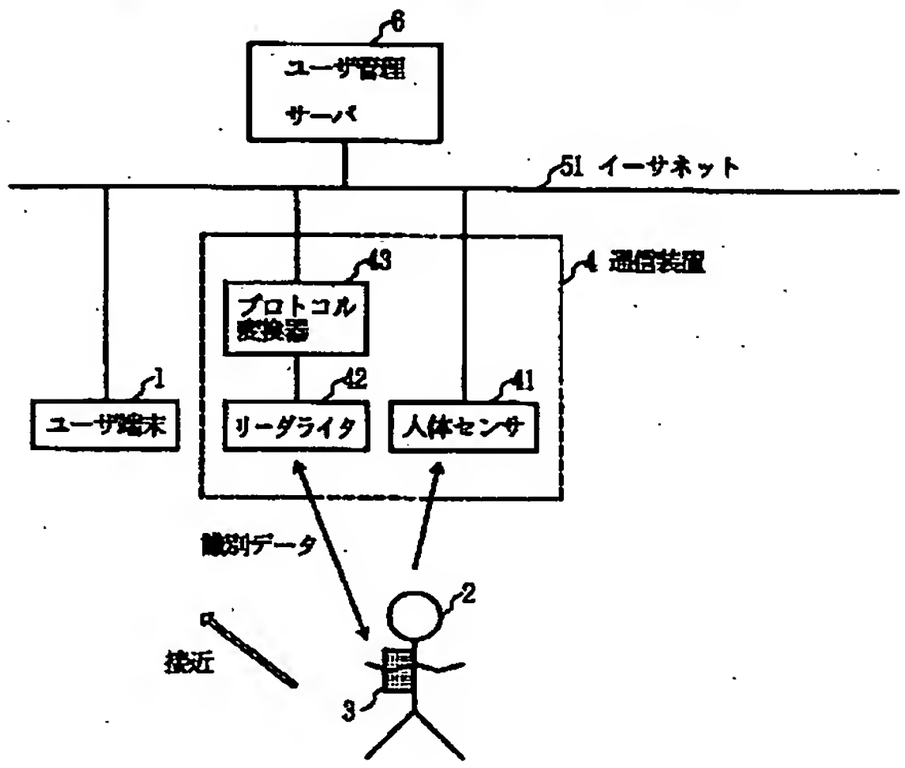
【図１】

本発明の無線タグを用いたユーザ認証システムの基本構成



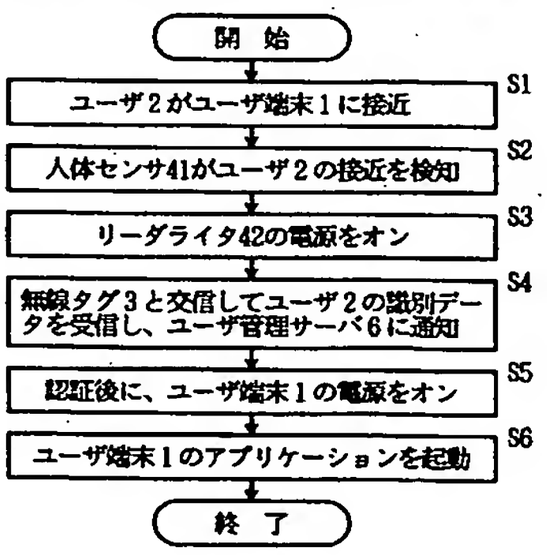
【図２】

本発明の無線タグを用いたユーザ認証システムの第１の実施形態



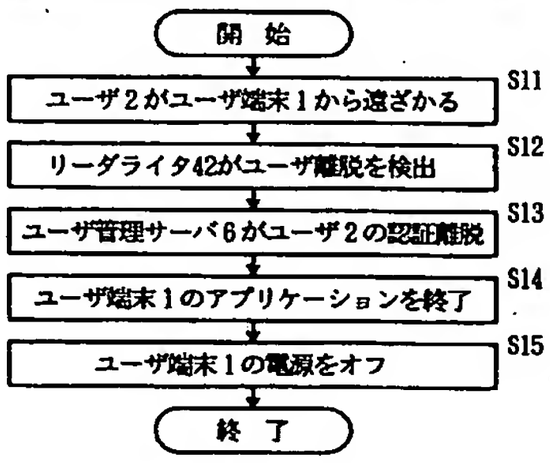
【図３】

ユーザの接近によるユーザ端末起動までの動作手順



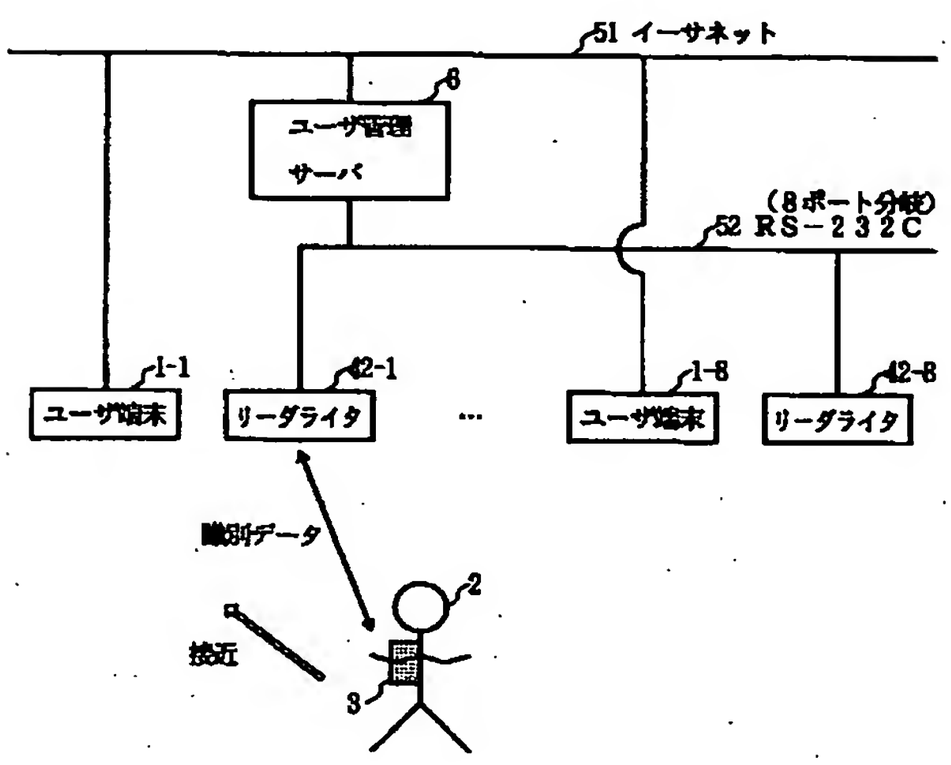
【図４】

ユーザの離脱によるユーザ端末起動停止までの動作手順



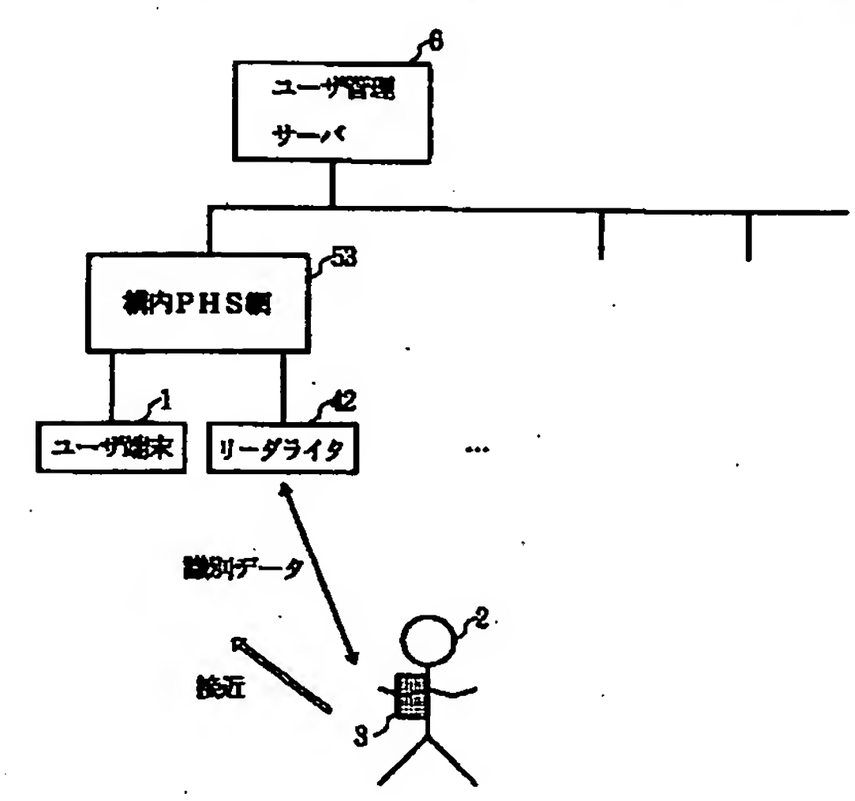
【図５】

本発明の無線タグを用いたユーザ認証システムの第２の実施形態



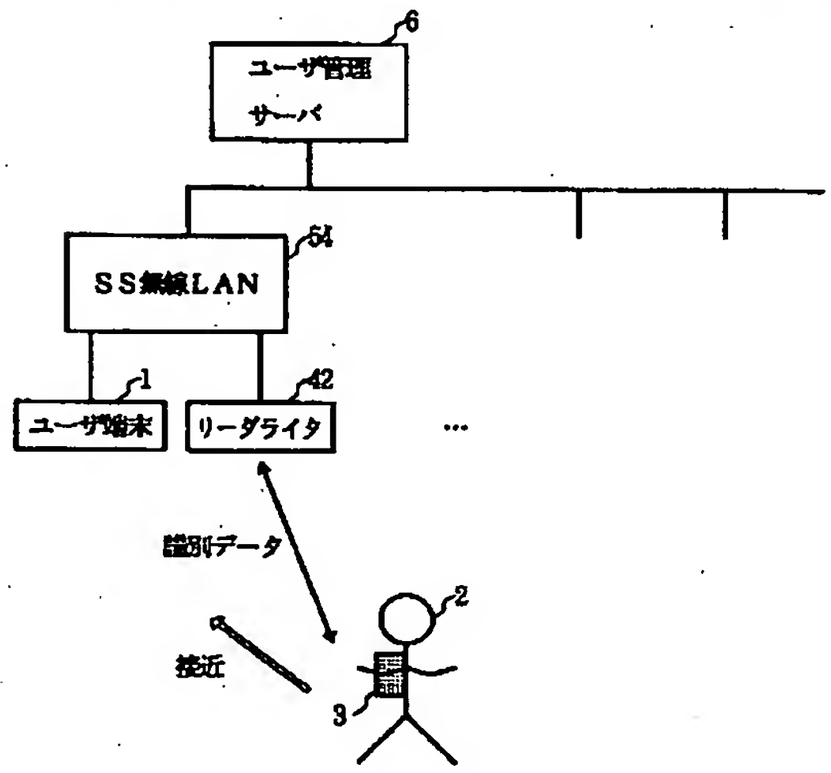
【図６】

本発明の無線タグを用いたユーザ認証システムの第３の実施形態



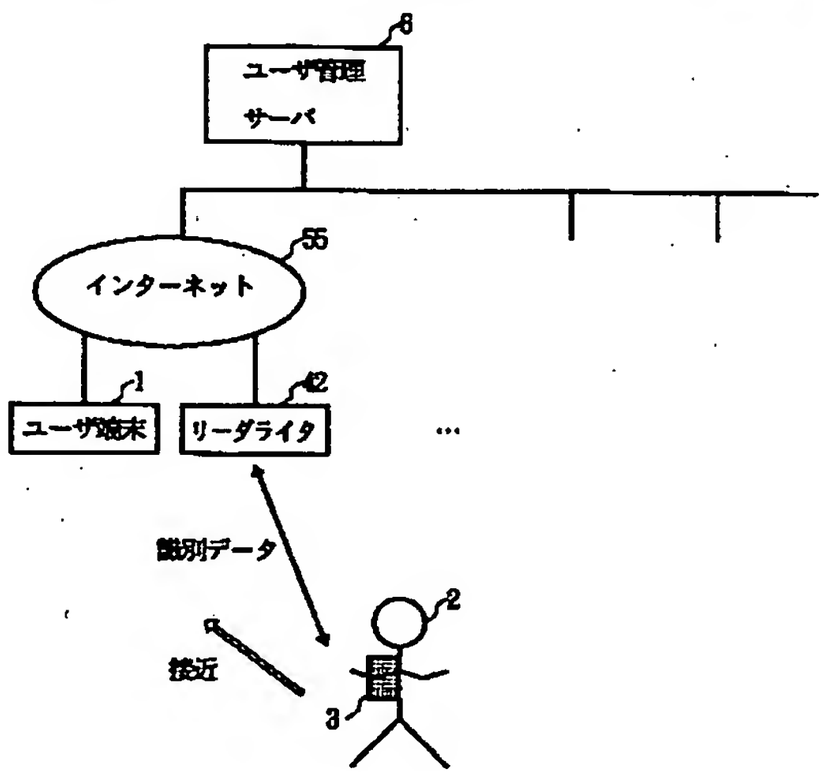
【図７】

本発明の無線タグを用いたユーザ認証システムの第４の実施形態



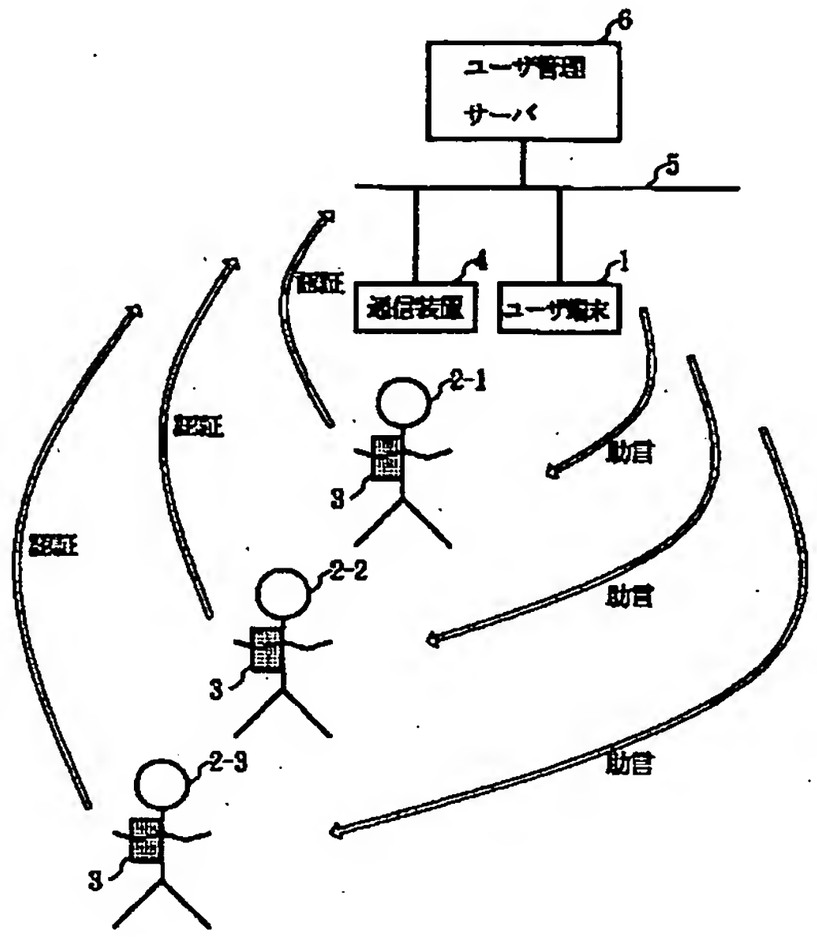
【図８】

本発明の無線タグを用いたユーザ認証システムの第５の実施形態



【図９】

本発明の無線タグを用いたユーザ認証システムの第６の実施形態



フロントページの続き

(51) Int. Cl.⁷	識別記号	F I		テーマコード（参考）
Ｇ０６Ｋ　19/07		Ｇ０６Ｋ　19/00	Ｈ	
19/00			Ｑ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	
			６７５Ｄ	

(72)発明者　三日月　哲郎
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B011 EA04 EA05 HH02 MA13 MA14 MA15
5B035 AA13 BB09 BC01
5B058 CA15 CA22 KA33 KA37
5B085 AA01 AE02 AE11 BC02
5J104 AA07 KA01 MA01 NA05